REMARKS

Reconsideration and allowance of the pending claims in the application are requested.

Claims 1-23 are pending in the case.

The Abstract has been objected to as exceeding the one hundred fifty word limit.

Claims 1-4 have been rejected under 35 USC 102(b) as being anticipated by Skinner et al., USP 5,963,914, issued October 5, 1999, filed December 9, 1997(Skinner).

Claims 5-7, 12-15, 17 and 23 have been rejected under 35 USC 102(e) as being anticipated by Bombard et al., USP 6,023,508, issued February 8, 2000, filed May 22, 1997 (Bombard).

Claims 8, 9 and 11 have been rejected under 35 USC 103(a) as being unpatentable over Bombard as applied to claim 5 above, and in further view of USP 6,549,210 to T. Van Hook, issued April 15, 2003, filed February 3, 1999 (Van Hook).

Claims 10 and 18 have been rejected under 35 USC 103(a) as being unpatentable over Bombard as applied to claims 5 and 13, and in further view of USP 6,662,167 B1 to J. Xaio, issued December 9, 2003, filed December 15, 1999 (Xiao).

Claims 16 and 19-21 have been rejected under 35 USC 103(a) as being unpatentable over Bombard., as applied to claim 13 above, and in further view of USP 5,768,385 to D. Simon, issued June 16, 1998 and filed August 29, 1995 (Simon)

Claim 22 has been rejected under 35 USC 103(a0 as being unpatentable over Bombard., as applied to claim 13 above, and in further view of USP 6,223,291 to L. Puhl issued April 24, 2001, filed March 26, 1999 (Puhl).

Before responding to the rejections, Applicants would like to distinguish Skinner, Bombard, Van Hook, Xiao, Simon and Puhl from the present invention (Jakobsson), as follows:

A. Skinner 5,963,914

Skinner discloses a method and system for automatically collecting and for analyzing information about time and work performed on a computer network which includes the following elements: a data collector for monitoring certain portions of a user's computer network activity and for logging into a log file those certain portions of a user's computer network activity; a data analyzer for determining by following user-defined rules showing which portions of those certain portions of a user's computer network activity constitutes continuous work activities, and how this work should be categorized by project and task with project; and an external interface for building the rules defining work. The data collector includes a resident module, such as a TSR (terminate-and-stay-resident) module, which extends the file system of the computer so that detailed records are kept of file activities. The data collector also routes information about file and keyboard activity, and tabulates and writes such information to a user's disk periodically. Skinner fails to disclose limitations of Jakobsson, as follows:

1. Skinner discloses a time tracking system for producing automatic documentation and unalterable proof of work done on a computer. **Skinner fails to disclose a certain amount of computational effort has been performed among a plurality of computational entities in a specified time interval as a Proof of Work to accomplish a separate, useful and verifiably correct computation.**

2. Skinner discloses a terminate-stay –resident module for data collection and analysis function of computer operation performed by an operator. **Skinner fails to disclose a computational entity performing a computational task by dividing the task into components; outsourcing different components to different computational entities for executionAnd collecting the responses from the different computational entities to accomplish the computational task.**

3. Skinner discloses a data analyzer reading a series of chronologically ordered events; categorizing the activities as belonging to a certain predetermined task; starting a timer when a task is detected, which stops after a preset idle time limit interval, and totaling the time for the task as a work period when the idle time has elapsed. **Skinner fails to disclose a Bread Pudding Protocol recycling**

computations from POW_2 for use in POW_1 reducing the computational burden in generating POW_1.

B. Bombard 6,023,508

Bombard discloses a system for transferring value carrying data packets representative of cash between transferor and transferee terminals without the intervention of a centralized database provides for data packets convertible between an inspected state and an uninspected state. Data packets in an inspected state can be negotiated between terminals once, whereupon they become uninspected and hence, non-negotiable. Uninspected data packets are restored to inspected state by having a central bank compare a hash code generated by a transferor terminal against a corresponding hash code generated by the central bank. Bombard fails to disclose limitations of Jakobsson, as follows:

1. Bombard discloses minting, which includes generating a data packet including an encrypted serial number representative of a cash note between a plurality of terminals and attaching it to an unencrypted cleartext record, which switches between a validation check number when the packet is in an inspected state and a transfer authorization number when the data packet is in an uninspected state. **Bombard fails to disclose minting coins based on a k-way hash function collision where a computationally entity is instructed to look within a pre-defined search space for "k" l-bit pre-images that hash to a range of y of l-bit images whose "t" least significant digits have the value "s" , where for security purposes, l is very large.**

2. Bombard discloses in negotiating the data packet for goods and services, a transferor uses a cryptographic algorithm and transfer authorization key of an inspected packet to generate a hash code which is stored in the transfer hash field of the transfer authorization number and in subsequent transfers the hash code is checked to be consistent with both a transferor authorization key found in a validation database and a negotiated value. **Bombard fails to disclose a plurality of computational entities, each generating a reply as a POW_1 which will be an l-bit pre-image that hashes to an l-bit image within a pre-defined range, and used by an entity 2 to achieve acceptance of POW_2 by entity 1.**

C. Van Hook 6,549,210

Van Hook discloses a method of generating cache indexes that reduces the likelihood that adjacent addresses will map to the same cache regions. The hashing process is optimized to be sensitive to small changes in the input data so that similar sets of input data will preferably not result in the same or even similar output data. Memory accesses of the sort performed when rendering graphical images may involve numerous accesses to relatively similar memory locations Therefore, hashing of the index values that determine where the information from the memory locations will be stored while that information is in cache decreases the likelihood of similar memory locations being stored at the same cache location. Consequently, cache efficiency and performance is improved. Van hook fails to disclose limitations of Jakobsson, as follows:

1. Van Hook discloses minimizing interaction between patterns of accessing cache memory for images and patterns of cache memory for storage. The bit information descriptive of an image is indexed and the index hashed. Hashing the index determines where the information will be stored and decreases the likelihood of similar information being stored at the same location. **Van Hook fails to disclose a hash function collision of pre-images or solutions that map to a single image, which is missing in Bombard. Van Hook hashing does the opposite of Jakobsson hashing.**

2. Van Hook discloses texture coordinates (s), (t) are both split into first and second portions, and provided to an XOR operation with the output concatenated to produce a hashed cache index. **Van Hook fails to disclose a hash function identifying images which collide within a pre-defined search space for "k" l-bit pre-images that hash to a range (y) of l-bit images whose "t" least significant bits have the value "s", where l is large for security purposes. Van Hook (s) and (t) coordinates are massaged for generating a hashed index and not the identification of images which collide for minting purposes, which is missing in Bombard.**

D. Xiao 6,662,167

Xiao discloses a method for solving partial constraint satisfaction problems in sequencing products for manufacture, such that the sequence produced is a near-optimal or optimal sequence, meaning that direct cost associated with various labor,

processes, and parts inventory are minimized and equipment and floor space utilization are maximized. One application of the method of the present invention is the sequencing of automobiles during manufacturing, in which vehicles are sequenced to go through a series of operations such as body forming, painting, component assembly (such as installing radios, seats, etc.) and final assembly (adding trim and chassis). Xaio fails to disclose limitations of Jakobsson, as follows:

1. Xaio discloses an evolutionary computation (EC) for solving real-world partial constraint satisfaction problems (PCSP). By repeating the computation for a population of chromosomes descriptive of potential solutions to the problem to be solved, a fitter population of chromosomes can be evolved. The best chromosome in the final population represents the optimal or near optimal solution to the problem. **Xaio fails to disclose transmitting a hash function to a plurality of computational entities conducting searches for images in different portions of a pre-image search space for bit values in the range of (y) of images whose "t" least significant bits have the value "s". Xaio repeats EC solutions to find the optimal solution and does not search in different search space for bit values that collide and represent a minted coin, which is missing in Bombard.**

E. Simon 5,768,385:

Simon discloses an electronic cash protocol including the steps of using a one-way function f.sub.1 (x) to generate an image f.sub.1 (x.sub.1) from a pre-image x.sub.1 ; sending the image f.sub.1 (x.sub.1) in an unblinded form to a second party; and receiving from the second party a note including a digital signature, wherein the note represents a commitment by the second party to credit a predetermined amount of money to a first presenter of the pre-image x.sub.1 to the second party. Simon fails to disclose limitations of Jakobsson, as follows:

1. Simon discloses a customer chooses a random number x_1 and uses f(x) to generate an image of x_1. The value x_1 is a random string obtained from a random number generator ....The customer keeps x_1 secret until a payment takes place and then it is sent as the payment. The customer withdraws a coin (non-anonymously) from the bank by requesting the bank associate a monetary value with $f(x_1)$. The bank complies by

digitally signing a statement to that effect , thus certifying $f(x_1)$as a valid coin and debits an account which customer maintains at the bank by the value of the coin. **Simon fails to disclose a coin consists of a k-way hash function collision, that comprises a set of pre-images or solutions that map to a single image. Simon forms a coin by a third party assigning a monetary value and digitally signing a statement as a valid coin, and not collecting images that map to a single image, which is missing in Bombard.**

2. Simon discloses that a customer wishes to anonymously exchange a coin, customer supplies to a bank x_1 and another image of the function $f(x_{2)}$ for some randomly chosen $x_{2..}$ The bank certifies $f(x_2)$ and keeps x_1 in a database as proof that $f(x_1)$ has already been spent. **Simon fails to disclose keying the hash function with a secret value that is only released on the issue date to prevent a potential forger from initiating effort prior to a given coin issue, which is missing in Bombard.**

F. Puhl 6,223,291:

Puhl discloses A wireless electronic commerce system (10) comprising a wireless gateway (18) to a wireless network (19) with which a wireless device (11) having a unique client identifier (ID) is capable of communicating. A server (15) or servers (15 and 16) is/are coupleable to the wireless gateway, delivering content items (e.g. software products) to the wireless device (11) and maintaining digital content certificates for content items and digital license certificates for licenses for the content items. The server maintains, for each wireless client associated with the system, a record of licenses for that client and a record of content items associated with each license.

1. Puhl discloses for systems not having a smart card, the keys and certificates are stored in a Wireless Identity Module software token. Member keys are protected by passphrase formation. This information is concatenated with a stored secret value for the device and run through a secure hash in order to generate the encryption/decryption keys for use in protecting the user private key. **Puhl fails to disclose a hash concatenation including a secret value specific to each coin to be minted and calculates a value y_i a pre-image value, x_i such that the concatenated hash value $(x_i , y_{i)}$ is equal to a target value "s". Puhl does not calculate a value**

representative of a pre-image for concatenation with a secret value in a hash function, which is missing in Bombard.

Summarizing, (1) Skinner fails to disclose harvesting a computational effort for a task from a computational entity which distributes the task among a plurality of sub-computational entities which generate POWs that are recycled into a POW response by the computational entity as a bread pudding protocol thereby reducing the computational burden of the computational entity; (2) Bombard fails to disclose minting coins based on a k-way hash function collision where a computationally entity is instructed to look within a pre-defined search space for "k" l-bit pre-images that hash to a range of y of l-bit images whose "t" least significant digits have the value "s" , where for security purposes, l is very large; (3) Van Hook fails to disclose a hash function collision of pre-images or solutions that map to a single image, missing in Bombard; (4) Xaio fails transmitting a hash function to a plurality of computational entities conducting searches for images in different portions of a pre-image search space for bit values in the range of (y) of images whose "t" least significant bits have the value "s", missing in Bombard; (4) Simon fails to disclose a coin consisting of a k-way hash function collision, that comprises a set of pre-images or solutions that map to a single image, missing in Bombard, and (5) Puhl fails to disclose a hash concatenation including a secret value specific to each coin to be minted and calculates a value y_i a pre-image value, x_i such that the concatenated hash value (x_i , y_i) is equal to a target value "s", missing in Bombard.

Applicants' submit the references have been overcome. The rejections of claims 1 -23 under 35 USC 102(b) and 35 USC 103 (a) fail for lack of support in the prior art. Withdrawal of the rejection and allowance of claims 1 -23 are requested.

Now turning to the rejection, applicants respond to the indicated paragraph of the office action, as follows:

REGARDING PARAGRAPHS 1 & 2:

The Examiner's comments are noted.

REGARDING PARAGRAPH 3:

The Abstract has been revised to be within 150 words.

The Examiner's remark with respect to the American Inventor's Protection Act of 1999 (AIPA) and the Intellectual Property high technology technical amendments' act of 2002 is noted.

REGARDING PARAGRAPH 4:

Claims 1-4 include limitations not disclosed in Skinner, as follows:

A. Claim 1:

(i) "a method of using a computational effort invested in proof of work (POW);"

Skinner discloses a time tracking system to produce automatic documentation of work done a computer. col. 2, lines 42-45. In contrast, Applicants disclose using a computational effort to convince and verify that a prover possesses knowledge of a secret or that a certain mathematic relationship holds true. Pg. 1, lines 1 – 9. Skinner fails to disclose a proof-of-work (POW) to accomplish a separate useful and verifiably correct computation.

(ii) "distributing a task among a plurality of entities."

Skinner discloses a data analyzer; a data collector; and an external interface perform the same task to each computer for monitoring and measuring the actual amount of work done on a computer by an operator. col. 2, lines 37-40. In contrast, Applicants disclose a computational task, which varies according to a desired computation, is distributed among computational entities for purposes of accomplishing a separate, useful and verifiably correction computation. pg. 1, line 4-16. Skinner discloses the same functional element performing the same computation and fails to disclose distributing portions of the same computation in processing as a proof of work.

(iii) "receiving a POW related to said task from one of said plurality of entities;"

Skinner, at col. 5, lines 36-62, discloses providing information about continuous activity as determined by each segment of user activity on a particular project, or task, exceeding an idle time interval. In contrast, Applicants disclose outsourcing the work related to a task to a plurality of entity. Each entity responds with a POW on completion of its component of work. pg. 3, lines 19-23. Skinner discloses selecting measured information from data processing elements, and fails to disclose POW replies relating to the assigned portion of the task performed by a computational entity.

(iv) "using said POW to accomplish said task."

Applicants can find no disclosure in Skinner relating to verifying and accomplishing a computation task, as described in the Applicants' specification at page 8, lines 8-15.

Skinner fails to disclose elements (i)-....(iv), described above and without such disclosure there is no support for the rejection of claim 1 under 35 USC 102(b). Withdrawal of the rejection and allowance of claim 1 are requested.

B. Claim 2:

Skinner, at col. 3, lines 19-22, discloses the data collected by the system can be encrypted to maintain the integrity of the data. In contrast, Applicants disclose POWs may be used to achieve a security goal, such as restrictive resource access, benchmarking, constructing of digital time capsules, and protection against spamming and other denial of service of text. pg. 8, lines 17-31.

C. Claim 3:

Skinner at col. 15, lines 34-56, discloses block 1208 gets the next activity and determines which task belongs to that particular activity. Block 1210 determines the owner of a particular activity. Block 1212 checks that the job or activity is not to be counted. In contrast, Applicants disclose distributing a plurality of sub-tasks to a respective one of a plurality of computation entities. The plurality of sub-tasks is directed to a computational event and not related to a particular activity performed on a

computer. Skinner fails to disclose distributing partitioned task to a plurality of entities.

D. Claim 4:

Skinner, at col. 4, lines 52-66, discloses an external interface for building rules to define work, including means for manually or automatically building the rules defining work. In contrast, Applicants disclose a security goal involves restricting resource access by one of said plurality of computation entities. pg. 8, lines 16-21. Skinner fails to disclose the subject matter of claim 4.

Summarizing, Claims 1-4 disclose limitations, as indicated above, not disclosed in Skinner. Without such disclosure in Skinner, there is no support in the prior art for the rejection of claims 1-4 under 35 USC 102(b). Withdrawal of the rejection and allowance of claims 1-4 are requested.

REGARDING PARAGRAPH 5:

Claims 5-7, 12-15, 17 and 23 include limitations not disclosed in Bombard, as follows:

A. Claim 5:

(i) " partitioning a minting operation into a plurality of subtasks;"

Bombard, at col. 3, line 9-21, discloses "the process of minting is typically performed by a central bank terminal at the request of another terminal, typically, an account custodian. The account custodian usually specifies the cash value of a data packet to be minted. The central bank then checks the account custodian credit. If the account custodian credit is deemed satisfactory, the central bank creates the data packet by assembling an encrypted record and a clear text record. The central bank then updates the data base to indicate that it has created a new data packet. In contrast, Applicants, at pg. 10, lines 6 -12 disclose partitioning a minting operation into a plurality of sub-tasks. Bombard fails to disclose the minting operation described at page 10, lines 6 -12

(ii) "distributing one of said plurality of sub-tasks to one of a plurality of entities;"

Bombard, at col. 5, lines 8-43, discloses the details of minting a data packet by a central bank. Applicants can find no disclosure in the cited reference regarding distributing the sub-task to a plurality of entities, as described in connection with the consideration of item (i), above. Bombard fails to disclose distributing one of the pluralities of sub-task to one of a plurality of entities.

(iii) "receiving a POW from said one of said pluralities of entities;"

Bombard, at col. 5, line 50 to col. 6, line 24, discloses the life-cycle of a data packet, as it circulates through a stream of commerce. The data packet does not represent at POW, wherein a prover demonstrates to a verifier a certain amount of computational work has been performed in a specified interval of time, as described in the specification at pg. 1, line 11-13. Bombard fails to disclose receiving a POW from one of the plurality of entities.

(iv) "using said POW to accomplish said mission operation;"

Bombard, at col. 5, line 50 continuing to col. 6, line 24, discloses an account custodian transmits a request for a data packet to a central bank. In response to this request, software executed by this central bank mints the requested data packet and transmits them to the account custodian. Applicants submit that the custodian request for data packets is not equivalent to a POW, describing a separate, useful and verifiably correct computation. Bombard fails to disclose using a POW to accomplish a minting operation.

Summarizing, Bombard fails to disclose the limitations of claim 5, for the reasons indicated above. Without such disclosure, there is no support in Bombard for the rejection of claim 5 under 35 USC 102(e). Withdrawal of the rejection and allowance of claim 5 are requested.

B. Claim 6 & 14:

Bombard, at col. 7, lines 24-33, discloses a central bank executes software instructions that verify that the account custodian is sufficiently credit-worthy to receive a data packet. Applicants submit for the reasons indicated in connection with the

consideration of claim 5 that a custodian request is not a POW to accomplish a security goal, as described in the specification at pg. 8, lines 16-23.

C. Claims 7 & 12:

Bombard, at col. 8, lines 25-53, discloses a negotiation method where a transferor uses a cryptographic algorithm and a transfer authorization key of the inspected data packet to generate a hash code. Subsequently, the hash code is used to generate a correct transfer authorization key and a negotiated value consistent with that found in a negotiated field of an uninspected data packet. In contrast, Applicants disclose transmitting a hash function to identify collisions occurring within a pre-defined search space that hashes to a range of images. pg. 11, lines 9-12. Bombard fails to disclose identifying valid solutions that hash to a predetermined image.

D. Claim 13:

(i) "distributing a minting operation among a plurality of entities in a manner that maintains privacy in said minting operations;"

Bombard, at col. 5, lines 8-43, describes a data packet having an encrypted record including a serial number; an original face value and means to identify the creator of the data packet and the terminal requesting the data packet. The data packet also includes a clear text record, which is unencrypted. The data packet can exist as an uninspected data packet and an inspected data packet. A transfer authorization key is used to convert a data packet in an inspected state to an uninspected state. Applicants can find no disclosure in Bombard distributing a minting operation through a plurality of entities for the reasons indicated in connection with the consideration of claim 3.

(ii) "using said POW to accomplish said minting operation."

Applicants can find no disclosure in Bombard for using said POW to accomplish said minting operations for the reasons discussed in connection with the considerations of claim 5.

Summarizing, claim 13 includes elements not disclosed in Bombard for the reasons indicated above. The rejection of claim 13 is without support in the prior art.

Withdrawal of the rejection of claim 13 under 35 USC 102(e) and allowance thereof are requested.

E. Claim 15:

Claim 15 is patentable over Bombard for the same reasons indicated in connection with the consideration of claim 7.

F. Claim 17:

Claim 17 depends from claim 15 and is patentable on the same basis as claim 15.

G. Claim 23:

Bombard, at col. 7, lines 24-33, discloses minting a data packet in response to a request from an account custodian. The minted data packet includes an encrypted cache serial number and a validation check number. Bombard fails to disclose a POW for reasons discussed in connection with the consideration of claim 5 and further fails to validate the POW, as described in the specification at pg. 8, lines 8-15.

Summarizing, rejection of claims 5-7, 12-15, 17 and 23 under 35 USC 102(e) fail for lack of support in the prior art. Withdrawal of the rejection and allowance of claims 5-7, 12-15, 17 and 23 are requested.

REGARDING PARAGRAPH 6:

Claims 8, 9 and 11 include limitations not disclosed in Bombard in view of Van Hook, as follows:

A. Claims 8 & 9:

The Examiner acknowledges that Bombard does not teach (1) that the predetermined image comprises a range of images, and (2) all images within the range of images have a predetermined number of least significant bits in common. Van Hook does not supply the missing elements in Bombard. Van Hook, at col. 9, lines 55-67, discloses hashing an index of coordinate values descriptive of an image where the hashed index value is used to map the memory locations in main memory. The locations are referred to by (s) "and (t) coordinates". The hashed index enables coordinates varying in only a few bits to be mapped to different locations in a cache memory. In contrast,

Applicants, at pg. 11, lines 8-12, disclose an entity transmits a hash function to be used in identifying collisions within a predefined search space for pre-images that have a range of images whose "t" least significant bits have the value "s". Van Hook hashes an index of coordinates for an image location and fails to disclose hashing the coordinates of a range of images that map to a single image.

B. Claim 11:

Bombard, at col. 2, lines 1-7, discloses a data packet representing a cache note exits in one of two circulation states. In a non-circulating state, transferring the data packet from one terminal to another is restrictive. In the circulating state, the data packet can exist in one of two inspection states. In one state, the packet can be freely transferred from one terminal to another and in another state, transferred to one terminal to another is restricted. In contrast, applicants at pg. 8, lines 16-24, disclose the computation and a POW may be used to achieve a security goal in restricting access, benchmarking, etc. Van Hook restricts the circulation of a data packet, whereas, applicants use the computation in a POW to achieve a security goal.

Summarizing, claims 8, 9 and 11, include limitations not disclosed in Bombard in view of Van Hook. Without such disclosure, there is no support for a worker skilled in the art to implement claims 8, 9 and 11. The rejection of claims 8, 9 and 11 under 35 USC 103(a) fails for lack of support in the prior art. Withdrawal of the rejection and allowance of claims 8, 9 and 11 are requested.

REGARDING PARAGRAPH 7:

Claims 10 and 18 include limitations not disclosed in Bombard, in view of Xiao, as follows:

The Examiner acknowledges Bombard does not teach each of the sub-tasks comprises searching a different solution space for a valid solutions. Xiao does not supply the missing elements in Bombard.

Xiao, at col. 2, lines 26-53 discloses the parameters for real-world scheduling/sequencing to accommodate different conditions and able to adapt to changes. Applicants can find no disclosure in Xiao relating to searching a different solution search

space for valid solutions, as described in the specification at pg. 11, line 20 continuing to pg. 12, line 5. The scheduling/sequencing problems and evolutionary computation used in resolving those manufacturing scheduling problems, does not disclose or suggest sub-task searching different solution search space for valid solutions. Without such disclosure, there is no basis for a worker skilled in the art to implement claims 10 and 18. the rejection of claims 10 and 18 under 35 USC 103(a) fails for lack of support in the prior art. Withdrawal of the rejection and allowance of claims 10 and 18 are requested.

REGARDING PARAGRAPH 8:

Claims 16 and 19-21 include limitations not disclosed in Bombard, in view of Simon, as follows:

A. Claims 16 & 19-21:

The Examiner acknowledges that Bombard does not teach that privacy is maintained in the minting operation by keying the hash value with a secret value or that the secret value includes portions specific to a coin or that the secret value includes a portion specific to a period of the coin validity. Simon fails to supply the missing elements in claim 16 and 19-21.

Simon, at col. 8, lines 65 to col. 9, line 15, discloses public keying encryption and the use of message authentication codes to ensure that messages between parties are not tampered with by someone other than the sender. Applicants can find no disclosure in Simon relating to using a suitable hash function and string concatenation, including a secret value, for generating a coin to be minted, as described in the specification at pg. 13, lines 3-14.

Simon, at col. 9, line 61, to col. 10, line 2, discloses refunding money when a user's smart card breaks and all of the keys are lost. The loser presents the key $f(x_i)$ within 3 month period to be credited with value of the coins. Simon fails to disclose keying a hash function with a secret key.

Claims 16 and 19-21 include limitations relating to (1) a predetermined numbers of valid solutions comprise a coin;(2) a hash function is keyed to a secret value; (3) the secret value includes a portion specific to a coin and (4) the secret value includes a portion specific to a period of a coin's validity, none of the foregoing limitations being disclosed or suggested in Bombard in view of Simon. Without such disclosure, a worker skilled in the art has no basis to implement claim 16 to 19-21. The rejection of claims 16 and 19-21 under 35 USC 103(a) fails for lack of support in the prior art. Withdrawal of the rejection and allowance of claims 16 and 19-21 are requested.

REGARDING PARAGRAPH 9:

Claim 22 includes limitations not disclosed in Bombard, in view of Puhl, as follows:

A. Claim 22:

The Examiner acknowledges that Bombard does not teach that the hash is of a concatenation of the solution and the value generated using the secret value. Puhl does not supply the missing element in Bombard.

Puhl, at col. 17, lines 24-42, discloses storing secret keys and member certificates in a wireless identity module software token. The member keys are protected by passphrase information. The information is concatenated with a secret value for the device and run through a secure hash in order to generate encryption/encryption key for use in protecting the user's private key. In contrast, applicants at page 13, lines disclose a hash function is concatenated with a secret value "r" specific to each coin to be minted. The computation performed aids in the successful completion of the task of finding the requisite number of pre-image values that hash to a specific range of images for the purpose of minting coins. Puhl discloses hashing for generating encryption/encryption keys and not for the purpose of minting coins.

Claim 22 includes limitations not disclosed in Bombard, in view of Puhl, as indicated above. Without such disclosure, there is no basis for a worker skilled in the art to implement claim 22. The rejection of claim 22 under 35 USC 103(a) fails for lack of

support in the prior art. Withdrawal of the rejection and allowance of claim 22 are requested.

PATENTABILITY SUPPORT FOR CLAIMS 24-28:

Claim 24 defines claim 1 in further detail and is patentable on the same basis. Claims 25-28 describe the limitations for determining when a proof of work is hard or feasible or sound.

Claims 24-28 further distinguish the present invention from the cited art. Entry and allowance of claims 24-28 are requested.

CONCLUSION:

Having provided a revised abstract; distinguished claims 1 – 23 from the cited art, and supported the patentability of new claims 24 – 28, applicants' request entry of the amendment, allowance of the claims and passage to issue of the case.

AUTHORIZATION:

The Commissioner is hereby authorized to charge any fees or insufficient fees or credit any payment or overpayment associated with this application to Deposit Account No. 13-4503, Order No. 3037-4166 BAALS 12-14.

Respectfully submitted,

MORGAN & FINNEGAN, L.L.P.

Dated: July 8, 2004

By: Joseph C. Redmond, Jr.

Joseph C. Redmond, Jr., Reg. No. 18,753
Telephone: (202) 857-7887
Facsimile: (202) 857-7929

CORRESPONDENCE ADDRESS:

Morgan & Finnegan L.L.P.
345 Park Avenue
New York New York 10154